IDA

INSTITUTE FOR DEFENSE ANALYSES

The Evolution Towards Decentralized C2

M.S. Vassiliou

January 2010

Approved for public release;
distribution is unlimited.

IDA Document NS D-4025

Log: H 10-000112

About this Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, Task AK-2-2701, "Net-Centric Tiger Team," for the Office of the Director, Defense Research and Engineering. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-4025

The Evolution Towards Decentralized C2

M.S. Vassiliou

We examine (1) the degree to which the U.S. military is planning to move towards a more decentralized C2 paradigm; (2) the adoption of such a paradigm by adversaries; (3) the degree to which the United States is actually making the transition; and (4) the factors enabling and impeding the shift. We find that many adversaries of the West, including terrorist organizations and "hybrid enemies," are already operating in an agile, decentralized manner. Meanwhile, top-level strategic plans of the U.S. Department of Defense (DoD) are consistent with a transition to net-enabled decentralized command and control (C2) for the U.S. military where appropriate, and the shift is supported by stated mission command doctrine. The transition is already occurring to some degree. In Afghanistan, for example, small Marine units operate with significant autonomy and edge-like behavior. The DoD has also made progress in the use of web-enabled collaborative systems. These systems have broadened information distribution and stimulated new interaction patterns, although they have not changed the allocation of decision rights. Technologies enabling the shift to net-enabled decentralized C2 must be coupled with appropriate policies and procedures and occasionally must overcome mid-level institutional cultural resistance.

Introduction

Alberts and Hayes (2006) have produced a succinct and effective categorization of approaches to command and control (C2). In their C2 "approach space," shown in Fig. 1, the dimensions are information distribution (tightly controlled or broadly disseminated); patterns of interaction between actors (tightly constrained or not); and allocation of decision rights (unitary or peer-to-peer). Classic, centralized, hierarchical C2 systems tend to have unitary allocation of decision rights, constrained patterns of interaction, and tightly controlled information flows. Networked (or "net-centric," or "net enabled") "edge organizations," on the other hand, tend to have a distributed allocation of decision rights, unconstrained patterns of interaction, and a broad dissemination of information.

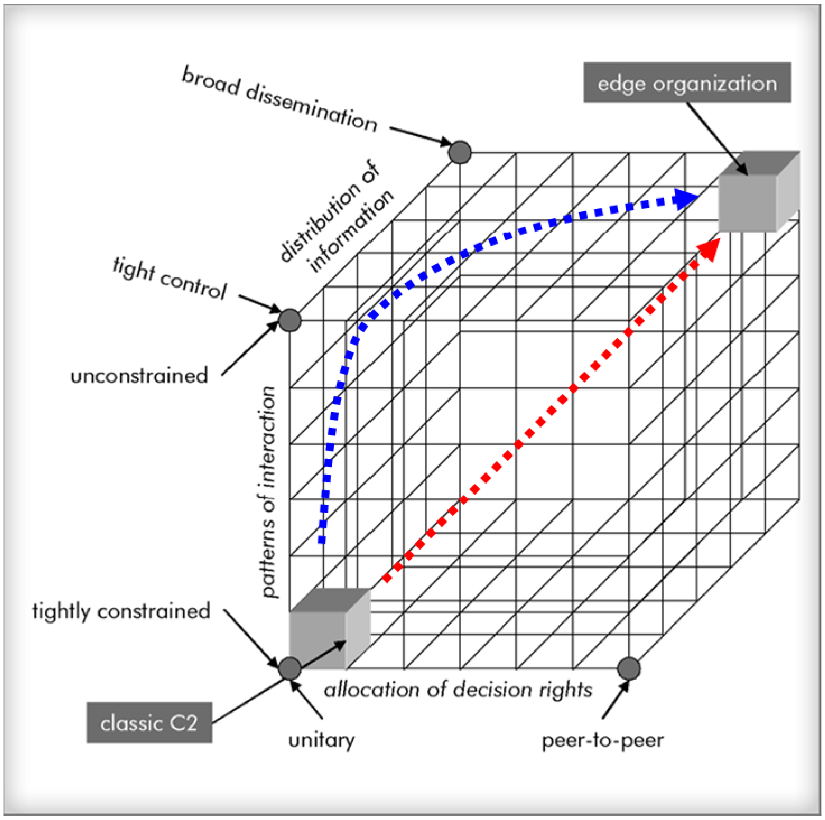


Fig. 1. The C2 Approach Space. (From Alberts and Hayes, 2006).

While centralized hierarchical C2 has been the dominant form since the onset of the Cold War, it is not necessarily the optimal model, particularly for emerging 21st century operations against a variety of agile adversaries. Experiments have shown that edge organizations can be better at solving problems than hierarchies[1]. In a hierarchy, information does not always migrate to where it is needed, when it is needed. Team leaders in hierarchies do not always act as brokers across organizational stovepipes. These factors have gained increasing recognition in the business world,[2] as large hierarchical

[1] Tan et al. (2009); Thunholm et al. (2009)

[2] Chambers (2009); Yardley and Kakabadse (2007)

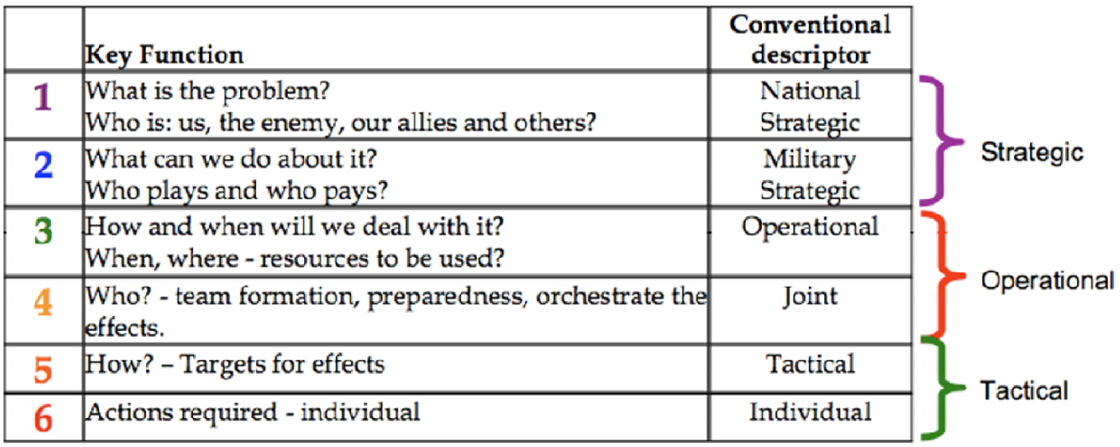
corporations have attempted to become more nimble in responding to rapidly changing market conditions. In some business intellectual circles, the very phrase "command and control" has become synonymous with a stultifying and bureaucratic approach. Admittedly, a number of businesses are paying mere lip service to a more decentralized approach to management, while retaining their rigid hierarchies. Others, however, appear to be achieving some degree of progress in implementing an "edge" approach.[3]

Alberts (2002) lists four tenets of network-centric warfare:

1. A robustly networked force improves information sharing.
2. Information sharing and collaboration enhance the quality of information and shared situational awareness.
3. Shared situational awareness enables self-synchronization
4. The above dramatically increase mission effectiveness.

Net-Centric Decentralized C2

Burgess and Fisher (2008) have developed a useful framework for thinking about net-centric, decentralized C2. They have delineated a number of generic command functions of varying levels of abstraction (Fig. 2). These can be disassociated from any particular hierarchical structures.



	Key Function	Conventional descriptor	
1	What is the problem? Who is: us, the enemy, our allies and others?	National Strategic	Strategic
2	What can we do about it? Who plays and who pays?	Military Strategic	
3	How and when will we deal with it? When, where - resources to be used?	Operational	Operational
4	Who? - team formation, preparedness, orchestrate the effects.	Joint	
5	How? – Targets for effects	Tactical	Tactical
6	Actions required - individual	Individual	

Fig. 2. Generic command functions. (From Burgess and Fisher, 2008).

In a traditional hierarchical, centralized C2 structure, the higher-level command functions are reserved for higher levels in the hierarchy, as shown in Fig. 3(a). When the level of abstraction of the command function does not correspond directly to a hierarchical level, various results are possible. Fig. 3(b) shows an example of the proverbial "6,000-mile long screwdriver," wherein an individual highly placed in the hierarchy is performing lower-level command functions and engaging with people much further down the chain. This type of micromanagement is not normally considered a desirable *modus operandi*, as it removes initiative from those closest to the situation at hand. Fig. 3(c) shows an

[3] Chambers (2009)

example of Charles Krulak's "strategic corporal in a three-block war."[4] The corporal performs many high-level command functions and autonomously directs his small unit. The strategic corporal and his small unit may be regarded as an instance of an edge organization. Fig. 3(d) shows a more complex web of command relationships, as might be conceived for a modern networked force. Note that the diagrams in Fig. 3 depict command relationships, and not just information flows. If Fig. 3(b), for example, were depicting information flows and not command relationships, it might not be indicative of micromanagement, but of a complex pattern of information sharing that may be desirable (e.g., as in the U.S. military's SKIWeb system discussed below).

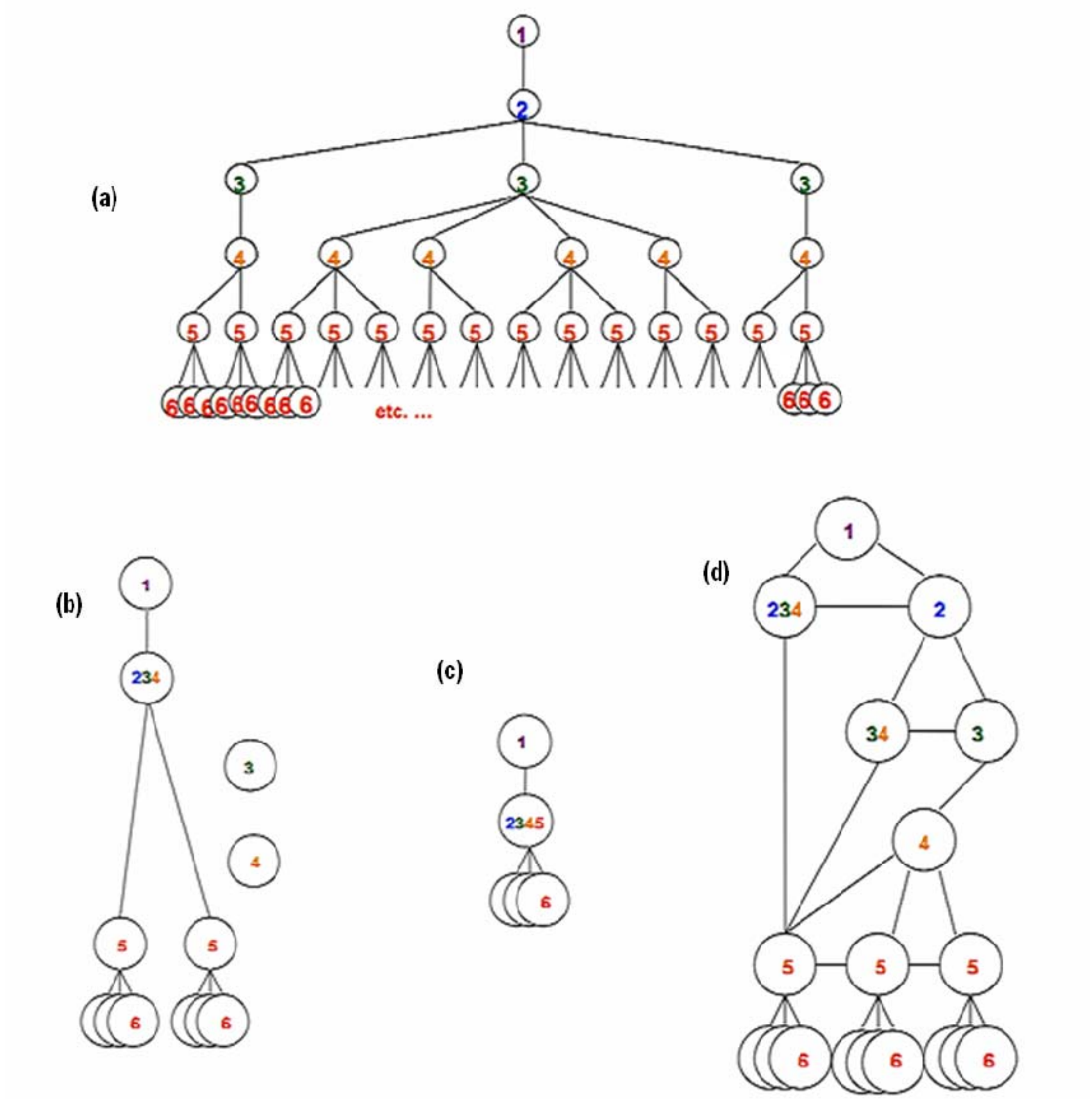


Fig. 3. Burgess and Fisher's (2008) generic command functions mapped to different command models: (a) Traditional centralized hierarchical structure; (b) Example of a micromanaged structure ("6,000 mile long screwdriver"); (c) Example of an autonomous small unit ("Strategic Corporal"); (d) Example of a modern networked force. (From Burgess and Fisher (2008).

[4] Krulak (1999)

Decentralized C2 is Observed Among Adversaries

Some potential adversaries of the West may have centralized, hierarchical C2 systems. Others, however, are arguably already behaving as edge organizations. This is particularly true of some terrorist networks. Al Qaeda, for example, appears to have executed the attacks of 11 September 2001 in a decentralized fashion.[5] Osama Bin Laden is thought to have known of the plan and blessed the operational concept at a high level, but he is not believed to have known the operational details, such as flight numbers. His subordinates understood his intent. They were trained and empowered to carry out the operation and fulfill that intent on their own. Al Qaeda operatives have shown a capability to self-synchronize, through unity of effort (a shared fundamentalist faith), a clear understanding of the commander's intent, and common rules of engagement. They have also made effective use of available information and communication technologies, employing the Internet and cell phones to develop shared awareness of intelligence and, ultimately, knowledge superiority. On September 11th, they knew their adversary better than their adversary knew them.

Some other terrorist organizations also show edge-like behavior. One example is the grassroots jihadi network responsible for the Madrid bombings of 2004.[6] Despite some weaknesses, the group managed to function in an autonomous and agile manner, without a continual need to consult senior levels. The network was an ad-hoc grouping with a complex leadership web, driven by a shared intent to carry out a terrorist bombing. Other examples of edge-like organizations include right-wing extremist groups in Germany and the U.S. In fact it was an American right wing extremist, Louis Beams, who enunciated the concept of "leaderless resistance."[7] Such groups, while not as apocalyptically successful as Al Qaeda, have made effective use of the Internet as a command and control medium.

Not all terrorist organizations or insurgencies behave as net-centric edge organizations. The "traditional" terrorist groups of the twentieth century, such as the Provisional Irish Republican Army (IRA) and the Basque separatist organization *Euskadi Ta Askatasuna* (ETA), had tighter hierarchical C2 architectures. The IRA and its splinter groups did move towards more edge-like behavior under pressure from law enforcement.[8] This is shown in Fig. 4.

It is sometimes stated that "It takes a network to defeat a network."[9] This seems like a reasonable assertion, although difficult to prove definitively. If an adversary organization's net-centric behavior makes it agile and flexible, it seems likely that one will be

[5] Zwikael (2007); Saunders (2002)

[6] Jordan et al. (2008)

[7] Jones (2007)

[8] Jackson (2006)

[9] e.g., Smith (2006)

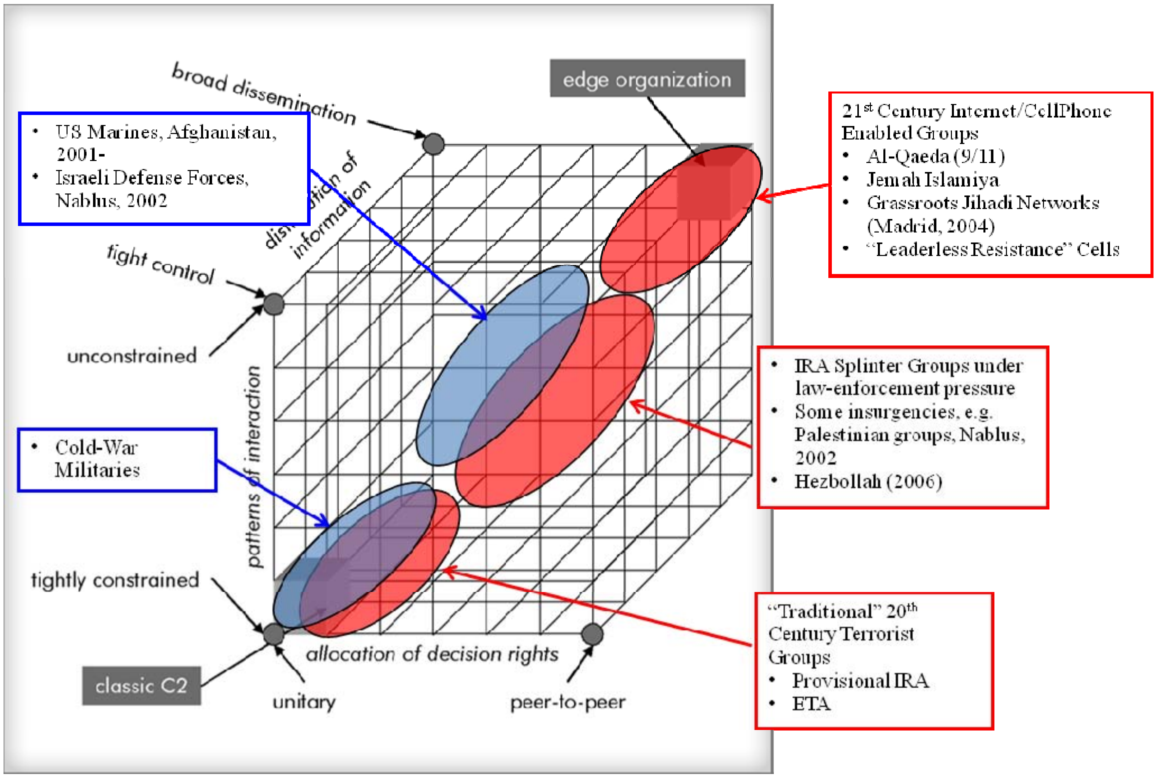

broad dissemination
edge organization
US Marines, Afghanistan, 2001-
Israeli Defense Forces, Nablus, 2002
distribution of information
tight control
unconstrained
Cold-War Militaries
patterns of interaction
tightly constrained
classic C2
allocation of decision rights
unitary
peer-to-peer
21st Century Internet/CellPhone Enabled Groups
Al-Qaeda (9/11)
Jemah Islamiya
Grassroots Jihadi Networks (Madrid, 2004)
"Leaderless Resistance" Cells
IRA Splinter Groups under law-enforcement pressure
Some insurgencies, e.g. Palestinian groups, Nablus, 2002
Hezbollah (2006)
"Traditional" 20th Century Terrorist Groups
Provisional IRA
ETA

Fig. 4. Estimated notional positions of some military and adversary entities in Alberts and Hayes's (2006) C2 Approach Space.

better positioned to defeat it if one also adopts those attributes. An instructive example may be found in the experience of the Israeli Defense Force (IDF) at Nablus in 2002.[10] The IDF faced a loose confederation of organizations including Hamas, Palestinian Islamic Jihad, some security forces from the Palestinian Authority, and street gangs. The groups coordinated with each other to a limited extent, but during the fighting they were autonomous and self-synchronizing. In order to fight them, the IDF formed small networks of its own, giving field commanders considerable autonomy. The small units exchanged information efficiently, both horizontally and vertically. The IDF engaged quickly and then withdrew, in a largely successful operation. The strategy required higher-level commanders to accept the autonomy of lower-level commanders, and required commanders in general to accept more questioning from subordinates.

The IDF's experience in the 2006 war with Hezbollah was not as positive. During this conflict, Hezbollah acted in a complex fashion, blending conventional and irregular warfare in a manner that has been labeled "hybrid."[11] The IDF's strategy involved conventional air operations, followed by a somewhat belated ground response when those did not fully succeed. Hezbollah's command and control had both hierarchical and distributed elements. There was apparently a formal chain of command, operating from command posts with fairly sophisticated equipment, including landline cables and

[10] Jones (2007)

[11] Jordan (2008)

encrypted radios.[12] However, Hezbollah also employed a distributed network of small units acting with considerable autonomy, displaying unity of effort and a degree of self-synchronization.[13] Hezbollah also used a somewhat decentralized media strategy, without the long message-approval cycles present in conventional militaries. Members understood the intended message and many were equipped with relatively inexpensive new media technologies enabling them to get it out fast, and significantly outflank Israel in the propaganda war.[14]

Top Level U.S. Strategic Vision Provides Support for Net-Enabled Decentralized C2

The National Defense Strategy of the United States, published in 2008, speaks of the need to counter a number of threats, including “violent, transnational, extremist networks.” It also speaks of the need to develop “concepts such as ‘net-centricity’,” and “to break down barriers and transform industrial-era organizational structures into an information and knowledge-based enterprise.”[15]

The top-level *Command and Control Strategic Plan* published by the United States Department of Defense (DoD) in 2009 also uses language consistent with a goal of transforming U.S. C2 to a more decentralized “edge-like” character:

> “Future C2 capabilities will reflect a paradigm shift in implementing C2 from the traditional centralized approach to one that emphasizes a distributed, collaborative, and cooperative net-enabled environment. C2 in this environment must possess the following attributes: interoperability, understanding, timeliness, accessibility, simplicity, completeness, agility, accuracy, relevance, robustness, and operational trust.”[16]

The C2 Strategic Plan seems at times to have a bit of a “senior commander” orientation. However, it does mention the need for “employing integrated capabilities that allow national leadership, commanders, and assigned forces to have visibility and easy access to information to effectively organize, understand, plan, decide, direct, and monitor the execution of operations, in support of a commander’s intent.” It also stresses the need for “a continued capability for decentralized decision-making in a hostile information environment as would exist after an attack disables the network.”[17] Further, it mentions the importance of considering the needs of users operating in difficult low-bandwidth environments.

Under the direction of the C2 Strategic Plan, the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer

[12] Biddle and Friedman (2008)

[13] Cordesman (2006); Rourke (2009)

[14] Collings and Rohozinski (2009)

[15] USDoD (2008)

[16] USDoD (2009a)

[17] USDoD (2009a)

(OASD (NII)/DoD CIO)) developed a C2 Implementation Plan outlining a broad action plan and execution responsibilities.[18] The DoD C2 Strategic Plan and the DoD C2 Implementation Plan taken together constitute the DoD C2 Roadmap, satisfying Department of Defense Directive (DoDD) 5100.30 (*DoD Command and Control*). The two plans also constitute the C2 Capability Portfolio Strategic Plan as required by Directive DoDD 7045.20 (*Capability Portfolio Management*).

Some Progress Towards Net-Enabled Decentralized C2 in the U.S. Military

While the U.S. DoD has not yet transformed its C2 architecture along the lines dictated by the C2 strategic plan, parts of the U.S. military are already behaving, at least to some extent, as edge organizations.

The United States Marines in Afghanistan are one example. In 2009 a marine regiment[19] might patrol a very large battlespace, possibly tens of thousands of square miles in size. Such a large area might formerly have been assigned to a whole division of several regiments. The 2nd Battalion, 7th Marines (2/7) alone conducted operations over 10,000 square miles in Afghanistan.[20] A battalion[21] was once the smallest Marine unit that would engage in independent operations; now a company[22] or even a platoon[23] may do this. The large responsibility and the dispersed nature of the adversary have resulted in a considerable amount of autonomy for small Marine units. They largely follow a relatively decentralized mission command doctrine.[24] The Marines are continuing to experiment with more decentralized C2, as in the Marine Corps Warfighting Laboratory's Distributed Operations (DO) concept, which later became Enhanced Company Operations (ECO). Experiments with more autonomous squads and platoons showed an increase in command speed, and a more rapid and effective engagement with adaptive adversaries.[25]

Various units of the U.S. Special Forces may also follow relatively decentralized C2 paradigms. Although little information is available in the open literature, one example can be found in the Special Forces "A-Teams" that began patrolling the Afghanistan-Pakistan border zone in 2001. Each comprised only about two dozen networked soldiers.[26] They operated in a highly autonomous manner, with distributed decision making. Each team had a person in charge of maintaining communications with the other teams. The Special Forces maintained a tactical web page containing information collected by the teams. Talbot (2004) recounts a case where a US Air Force plane noticed vehicle lights, and relayed the information to the webmaster, who then communicated

[18] USDoD (2009b)

[19] Around 4,000–5,000 marines, but this can vary

[20] Price and McHuen (2009)

[21] Notionally about 300–500 marines, but can be more. The 2/7 has about 800 troops.

[22] Notionally about 110 marines

[23] Notionally about 36 marines

[24] Conversation with a U.S. Marine major

[25] Price and McHuen (2009); Goulding (2009)

[26] Talbot (2004)

with the dispersed Special Forces teams. One team was able to investigate and get information back to nearby planes, leading to the destruction of a Taliban column.

Doctrine is not Necessarily an Obstacle: Mission Command

In various conversations with personnel from the U.S. DoD about the possibility for net-enabled decentralized C2, we have sometimes heard the assertion that such a vision for C2 may have difficulties because it goes "against established doctrine." However, an examination of various doctrinal publications suggests that doctrine is not necessarily an obstacle. Many Western military establishments, including that of the United States, have adopted some form of mission command as part of their stated doctrine.

Mission command is not synonymous with net-enabled decentralized C2, and does not in itself guarantee the development of edge organizations. However, mission command can provide a fertile soil from which edge organizations may grow; and net-centric technologies can in turn be used to facilitate mission command.

In mission command, commanders are expected to issue only the most essential orders, providing objectives and general instructions, and establishing command intent. Subordinates have considerable autonomy to develop tactical details suited to the particular real situations they face. While detailed, strictly hierarchical C2 seeks—perhaps in vain—to reduce battlefield uncertainty, mission command embraces the uncertainty and empowers subordinates to deal with it.

In the United States, Army publication Field Manual (FM) 6-0 "establishes mission command as the C2 concept for the Army."[27] The publication further states:

> "Mission command relies on subordinates effecting necessary coordination without orders. While mission command stresses exercising subordinates' initiative at the lowest possible level, all soldiers recognize that doing so may reduce synchronization of the operation. Thus, commanders accept the uncertainty that accompanies subordinates exercising initiative. Their trust in subordinates they have trained gives them the assurance that those subordinates will direct actions that will accomplish the mission within the commander's intent."

The United States Marine Corps has also established mission command as its official doctrine:

> "The Marine Corps' concept of command and control is based on accepting uncertainty as an undeniable fact and being able to operate effectively despite it. The Marine Corps' command and control system is thus built around mission command and control which allows us to create tempo, flexibility, and the ability

[27] USArmy (2003)

> to exploit opportunities but which also requires us to decentralize and rely on low-level initiative."[28]

> "Mission command and control tends to be decentralized, informal, and flexible. Orders and plans are as brief and simple as possible, relying on subordinates to effect the necessary coordination and on the human capacity for implicit communication—mutual understanding with minimal information exchange. By decentralizing decision-making authority, mission command and control seeks to increase tempo and improve the ability to deal with fluid and disorderly situations."[29]

The U.S. Marines even go so far as to caution against procuring any equipment that would enable an interference with mission command:

> "Equipment that permits over control of units in battle is in conflict with the Marine Corps's philosophy and is not justifiable."[30]

When officers from the First Battalion, 2nd Marines (a unit with extensive combat experience in Iraq) were interviewed by researchers from the Naval Postgraduate School about operational and technological needs, they had a "hesitancy to embrace any technology that would allow those higher echelons the temptation of micro-managing small unit actions from behind a plasma screen."[31]

The United States Air Force does not explicitly enunciate a mission command doctrine, but does observe that a "reluctance to delegate decisions to subordinate commanders slows down C2 operations and takes away the subordinates' initiative."[32]

In the United Kingdom, mission command is a stated cornerstone of defense policy.[33]

> "The United Kingdom's philosophy of command is based on mission command, which promotes initiative, decentralised command, and freedom and speed of action, yet remains responsive to superior direction."[34]

The UK also makes an explicit connection between mission command and net-enabled capability (NEC):

> "… increasing degrees of NEC permit mission command to be extended, with confidence, down through the tiers of command."[35]

[28] USMC (1996)

[29] USMC (1996)

[30] USMC (1989)

[31] Senn and Turner (2008)

[32] USAF (2007)

[33] UKArmy (2005); UKMod (1989); UKRAF (2008)

[34] UKRAF (2008)

[35] UKRAF (2008)

Mission command is also important in Canadian doctrine,[36] Dutch doctrine,[37] and many others.

But Doctrine is not Enough

The adoption of a doctrine embracing mission command and tenets of decentralized C2 may be necessary for those militaries that wish to implement such concepts, but it is not sufficient. Moving from a centralized, hierarchical C2 paradigm to a more decentralized one, even in only a subset of situations, requires considerable effort in changing the command culture. Higher levels of command must become accustomed to delegating and not over-specifying or micromanaging missions. Lower levels must become accustomed to taking initiative and not receiving highly detailed orders.

Although instances of decentralized command have occurred throughout history, modern notions of mission command have their roots in nineteenth century Prussia.[38] During the Napoleonic wars, the orthodox, highly centralized and hierarchical Prussian army suffered defeats from a more freewheeling French adversary, whose soldiers and officers were perhaps less professional, but more agile and flexible. The defeats led to an intensive review of the Prussian army and its practices, and resulted in a change in the 1788 Prussian Field Service Regulations in 1837. The changes established the notion of command intent, and the duty of subordinates to interpret and understand it. A further change in the regulations in 1869, under the influence of Helmuth von Moltke, established that orders should only be as detailed as absolutely necessary. By 1888 the German army had fully adopted what we understand as mission command. "Mission Command" is actually a translation of *Auftragstaktik*, the German name for the concept. *Auftragstaktik* contributed considerably to German successes in the early part of the Second World War. The point of all this is that the German doctrine and its application took a century to evolve, allowing a thorough inculcation of the mission command concepts of trust and simple orders into the military culture.[39]

Simply "cutting and pasting" mission command concepts into doctrine is unlikely to yield successful results.[40] It has been observed, for example, that the British Army in the Second World War was theoretically working from a fairly decentralized doctrine, but did not behave accordingly and did not reap the associated benefits.[41] Stewart (2006) quotes other observers who noted that the Germans and Italians had similar doctrine in that war, but achieved very different levels of success, probably owing to military cultural factors. Stewart (2006) discusses a number of examples of military organizations with mission-command doctrines behaving in a hierarchical and centralized fashion, depending in part on the personalities of individual commanders. Stewart (2009)

[36] Canada DND (1996)
[37] Vogelaar and Hanskramer (2004)
[38] Yardley and Kakabadse (2007)
[39] Wyly (1991)
[40] Oliveiro (1998)
[41] Johnston (2000)

summarizes a number of studies showing significant variations in the importance accorded to understanding command intent—an essential aspect of mission command—by officers of doctrinally decentralized Western military organizations.

Even in a military organization with a mission-command doctrine, commanders with a tendency to micromanage may do so if the general culture allows it. The same technologies that facilitate decentralization and the transmission of intent can sometimes also facilitate micromanagement. Zagurski (2004) notes that in some early U.S. Army experiments with fully digitized brigade combat teams, some commanders attempted to micromanage. In its Fleet Battle Experiments-India (FBE-I) of 2001, the U.S. Navy tested decentralized execution of joint fires. The experiments showed that operational commanders often have considerable difficulty allowing decentralized execution.[42] In the real world, the pressure to micromanage can be significant, given the visibility of modern tactical operations to upper command echelons and the media.[43]

Web-Enabled Collaborative Technologies

One area where the U.S. DoD has made some impressive progress is in the use of web-enabled collaborative technologies for C2 and administration. Such capabilities use the worldwide web (or, in the case of the military, a secure subset thereof) as a platform for software applications, user interaction, and dynamic information sharing. They have come to be known collectively as "Web 2.0"[44] (although one could reasonably argue that the web was always intended to be used in this way). Below we consider some examples of web-enabled collaborative systems in the military. As we shall discuss in the next section, such systems do not represent full transformation to "edge C2." They neither require mission command nor do they necessarily facilitate it. They are nonetheless important, because of the breadth of information distribution that they enable, and the often nonhierarchical manner in which the information moves.

Knowledge Web

Knowledge Web, or KWeb[45], is a collaborative technology adopted on the USS *Carl Vinson* and Carrier Group 3 under the command of Rear Admiral Thomas Zelibor, after testing during Global Wargame 2000. KWeb created a battle-group website for shared situational awareness over SIPRNet. Tactical action officers were able to post and obtain critical time-sensitive information via Secure Chat. Various web pages provided the equivalent of a dynamic status board, and the speed of command was no longer tied to the briefing cycle. Before KWeb, operations staffs would work into the night preparing for briefings. This was no longer necessary, and commanders could brief from the dynamically updated web pages rather than creating separate PowerPoint charts. Staff meetings no longer dwelled on status updates, and instead concentrated on more crucial

[42] Saunders (2002)

[43] Fox (1995); Ramshaw (2007)

[44] Graham (2005)

[45] Doyne et al. (2006); Stulberg (2009).

strategy and tactics. As it happened, Carrier Group 3 reached the Arabian Sea on the eve of the September 11, 2001 attacks, and was transformed into Carrier Task Force 50 (CTF-50), eventually including nearly 60 ships from several coalition nations. CTF-50 played a part in Operation Enduring Freedom (OEF). The time saved by using KWeb permitted more and better contingency planning during OEF.

As time went on, the Navy integrated KWeb into a larger C2 framework for the whole service, and the exigencies of integration unfortunately made KWeb somewhat more difficult to use. In addition, the departure of Admiral Zelibor meant the loss of a champion. Other commanders showed varying degrees of enthusiasm for the system. Some preferred the old way of doing things. The successor to KWeb is now sometimes used and sometimes not, largely depending on commander personality and preferences, but also on technical factors such as available bandwidth.[46]

SKIWeb

The Strategic Knowledge Integration Web (SKIWeb) is a web-based asynchronous collaboration system introduced at the United States Strategic Command (STRATCOM) under the leadership of General James Cartwright.[47] At the end of 2009, the system had 28,000 users throughout the DoD, at all levels of command.[48] Any user, from a general to a front-line soldier, can post information, and that information is accessible to all. Users can also expand, correct, and comment on others' posts. The system stimulates a non-hierarchical flow of information. As General Cartwright said,

> "The metric is what the person has to contribute, not the person's rank, age, or level of experience. If they have the answer, I want the answer. When I post a question on my blog, I expect the person with the answer to post back. I do not expect the person with the answer to run it through you, your OIC [Officer-in-Charge], the branch chief, the exec, the Division Chief, and then get the garbled answer back before he or she posts it for me."[49]

SKIWeb's primary function is to inform the middle and upper layers of command. Although anyone can post, event postings are typically made by action officers and are read by both lower and higher levels. Higher-level officers might typically also blog on certain events, asking questions or adding information and perspective. SKIWeb is generally regarded as a success that has increased the timeliness and relevance of information and expanded situational awareness at all levels of command. Recent examples where it has proved useful include quick-reaction monitoring of Russian flights near Alaskan airspace, and monitoring incidents of piracy near Somalia. Since piracy occurs in an area straddling the boundary of CENTCOM and AFRICOM jurisdictions, a DoD-wide situational awareness system is particularly useful.

[46] Personal conversations with individuals involved in KWeb development

[47] Cartwright (2006); Wyld (2007); Soknich (2009)

[48] Personal communication from a USSTRATCOM official

[49] Defense Industry Daily (2005)

The development of SKIWeb was not just the result of department-wide policy, but depended crucially on the unique personality and efforts of General Cartwright. The system met considerable internal cultural resistance at first. Implementation was initially hampered by several objections from computer security personnel. There was also initial resistance to the idea that lower echelons could share information directly with the general. Since the general himself was behind the concept, however, objections were overcome.[50] While SKIWeb would probably not have been launched without General Cartwright, it has now transcended him and has survived and expanded since his departure from STRATCOM.

Despite the possibility that a technology such as SKIWeb might facilitate micromanagement of remotely deployed units, we uncovered no evidence that this ever occurred in practice.

CAVNET

Our final example comes from the tactical domain. CAVNET is a web community associated with the U.S. First Cavalry in Iraq, used by junior officers to share important mission-related information. In one publicized use of the network, a patrol leader in Baghdad learned that insurgents were wiring posters of Moqtada al-Sadr to explode when U.S. soldiers took them down, and posted the information. Another officer elsewhere in the city read the information and alerted his soldiers, who discovered some of the rigged posters and safely removed them.[51]

Technological Trajectories

Fig. 5 illustrates possible trajectories for technologies in C2 and related areas. Some technologies (Fig. 5 (A)) may be used to make traditional hierarchical systems function better and faster. One might argue that most C2 technologies of the last several decades fall into this category. The introduction of computerized systems where none existed before, for example, may have had such an effect. This was followed by the continual improvement of those systems and increasing richness in the data conveyed. The basic hierarchical, centralized mode of doing business did not change.

Other technologies (Fig. 5 (B)) may facilitate information distribution to some hitherto unanticipated degree, and inspire changes in policy towards broader distribution.[52] In so doing they may stimulate an expansion in interaction patterns.[53] However, the allocation of decision rights may still be unchanged. The Web 2.0 technologies discussed above—as currently applied in the DoD—fall largely into this category. SKIWeb, for example, has

[50] Personal conversations with STRATCOM personnel

[51] Baum (2005)

[52] Alternatively, they may be inspired by such policy changes.

[53] Or they may sometimes result from such an expansion.

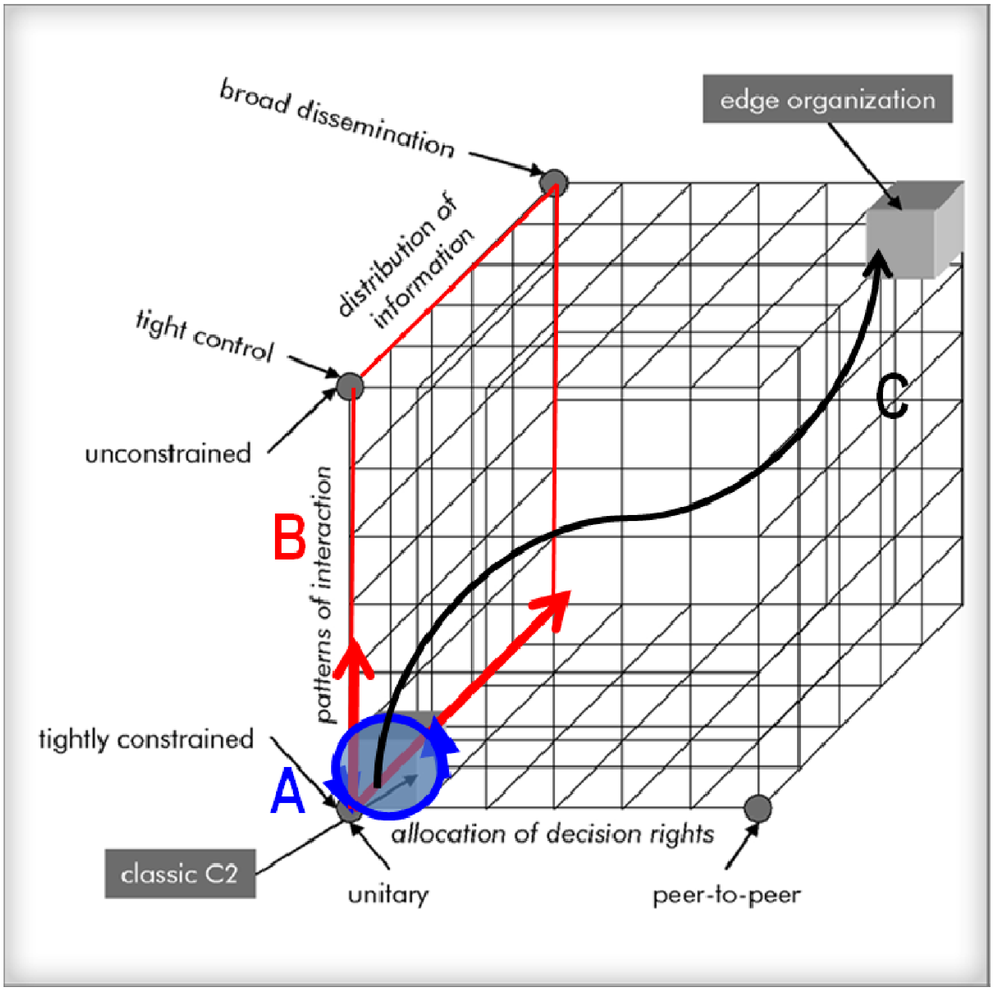
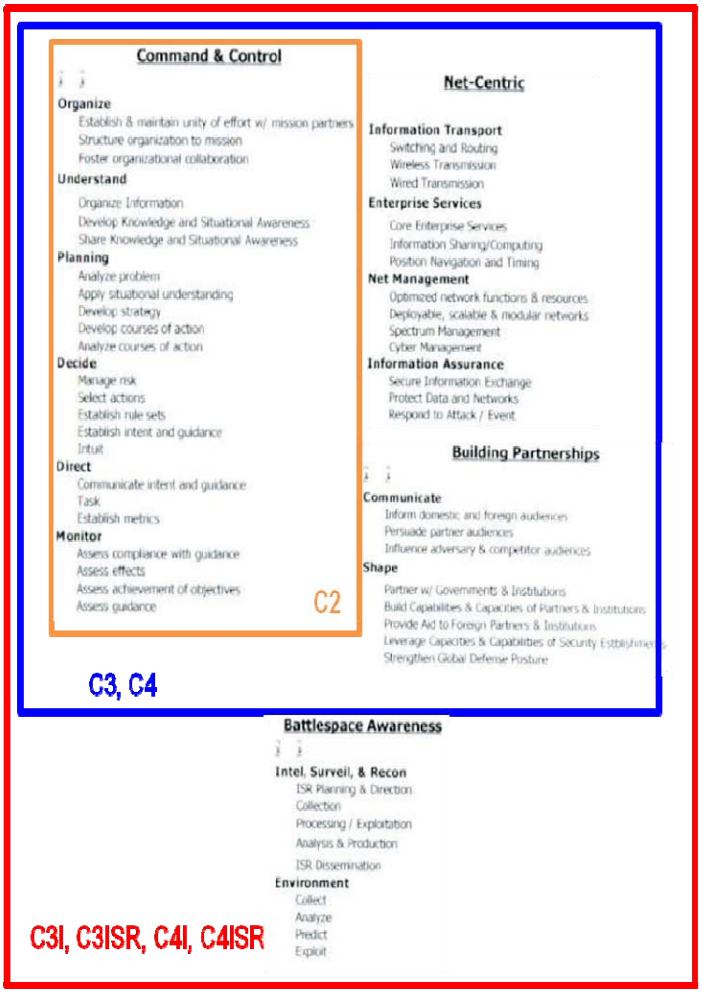


Fig. 5. Technological trajectories superimposed on the C2 Approach Space of Alberts and Hayes (2006). Some technologies (A) may be used to make traditional hierarchical systems function better and faster. Other technologies (B) may facilitate information distribution and inspire (or be inspired by) changes in policy towards broader distribution. In so doing they may stimulate an expansion in interaction patterns, or sometimes result from such an expansion. However, the allocation of decision rights may still be unchanged. Some technologies (C), coupled with policy and culture changes, can facilitate the transition to an edge organization. In some cases the same set of technologies may fall into any of the three categories, depending on how it is used.

clearly changed the patterns of interaction between the actors in the system: action officers now post information that is seen by a four-star general, who may then ask direct questions. By the same token, information is very broadly disseminated across the network. However, the basic hierarchical structure remains fully intact.

Some technologies (Fig. 5 (C)), coupled with the appropriate policy and culture, can facilitate the transition to an edge organization. As an example, consider the area of communications technology for dispersed tactical units. Small units operating in remote expeditionary environments could benefit greatly from data bandwidth comparable to that available in forward operating bases, particularly if this could be achieved without requiring the unit to carry and deploy bulky equipment such as dish antennas. Such a high-bandwidth communications capability, coupled with an effective application of some of the new small-unit concepts being tested by the U.S. Marines—or a reasonable application of existing mission command doctrine—could help create an effective edge organization in the field. The same could be said for secure mobile ad hoc networks of lightweight handheld multimedia devices. Local intelligence, surveillance, and reconnaissance (ISR) assets such as small drones, effectively integrated into the mobile communications architecture, are another example of an enabling technology.

It is worth observing that many of the technologies necessary for the transition to net-enabled "edge" C2 do not fall neatly into the area labeled "C2." This is perhaps one reason for the emergence of a bewildering array of terms to indicate a "greater C2:" Command, Control, and Communications (C3), Command, Control, Communications, and Computers (C4), Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), etc. An examination of the United States Joint Staff's (2008) nine Joint Capability Areas reveals that Command and Control and closely related areas encompass four of them. These are shown in Fig. 6.



Command & Control
Organize
Establish & maintain unity of effort w/ mission partners
Structure organization to mission
Foster organizational collaboration
Understand
Organize Information
Develop Knowledge and Situational Awareness
Share Knowledge and Situational Awareness
Planning
Analyze problem
Apply situational understanding
Develop strategy
Develop courses of action
Analyze courses of action
Decide
Manage risk
Select actions
Establish rule sets
Establish intent and guidance
Intuit
Direct
Communicate intent and guidance
Task
Establish metrics
Monitor
Assess compliance with guidance
Assess effects
Assess achievement of objectives
Assess guidance
C2
Net-Centric
Information Transport
Switching and Routing
Wireless Transmission
Wired Transmission
Enterprise Services
Core Enterprise Services
Information Sharing/Computing
Position Navigation and Timing
Net Management
Optimized network functions & resources
Deployable, scalable & modular networks
Spectrum Management
Cyber Management
Information Assurance
Secure Information Exchange
Protect Data and Networks
Respond to Attack / Event
Building Partnerships
Communicate
Inform domestic and foreign audiences
Persuade partner audiences
Influence adversary & competitor audiences
Shape
Partner w/ Governments & Institutions
Build Capabilities & Capacities of Partners & Institutions
Provide Aid to Foreign Partners & Institutions
Leverage Capacities & Capabilities of Security Estblishments
Strengthen Global Defense Posture
C3, C4
Battlespace Awareness
Intel, Surveil, & Recon
ISR Planning & Direction
Collection
Processing / Exploitation
Analysis & Production
ISR Dissemination
Environment
Collect
Analyze
Predict
Exploit
C3I, C3ISR, C4I, C4ISR

Fig. 6. Command and Control (C2) and closely related areas encompass four of the nine Joint Capability Areas developed by the United States Joint Staff (2008).

Conclusions

- Following Alberts (2002), a net-enabled, decentralized implementation of C2 can improve information sharing, collaboration, and situational awareness, thereby enabling self-synchronization and increasing mission effectiveness.
- Many adversaries of the West, including terrorist organizations and "hybrid enemies," are already operating in an agile, decentralized manner.
- Top-level strategic plans of the U.S. DoD are consistent with a transition to net-enabled decentralized C2 for the U.S. military where appropriate.
- The shift is supported by stated mission command doctrine.
- However, doctrine is not enough, and must be accompanied by an appropriate institutional culture.
- The transition is already occurring to some degree. In Afghanistan, for example, small Marine units operate with significant autonomy and edge-like behavior.
- The DoD has made considerable progress in the use of web-enabled collaborative systems. These systems have broadened information distribution and stimulated new interaction patterns, although they have not changed the allocation of decision rights.
- Technologies enabling the shift to net-enabled decentralized C2 must be coupled with appropriate policies and procedures, and occasionally must overcome mid-level institutional cultural resistance.

Acknowledgements

This work was performed under Institute for Defense Analyses Contract No. W91WAW-09-C-000, task order AK-2-2701. I thank David Jakubek, Jon Agre, Caroline Ziemke-Dickens, and Rob Mahoney for helpful discussions.

References

Alberts, David (2002). *Information Age Transformation: Getting to a 21st Century Military*. Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org

Alberts, David S., and Richard E. Hayes (1995). Command Arrangements for Peace Operations. Washington, D.C.: National Defense University Press. Available at www.dodccrp.org.

Alberts, David, and Richard E. Hayes (2006). Understanding Command and Control. Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org

Baum, Dan (2005). "Battle Lessons." *The New Yorker*, 17 January.

Biddle, Stephen, and Jeffrey A. Friedman (2008). *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy*. Carlisle, Pennsylvania: U.S. Army War College, Strategic Studies Institute.

Burgess, Alan and Peter Fisher (2008). *A Framework for the Study of Command and Control Structures*. Edinburgh, South Australia: Commonwealth of Australia Defense Science and Technology Organization, Publication DSTO-TN-0826.

Canada DND (Department of National Defence) (1996). *Conduct of Land Operations – Operational Level Doctrine for the Canadian Army*. Publication B-GL-300-001/FP-000. Ottawa, Ontario: Queen's Printer.

Cartwright, James E. (2006). "Information Sharing is a Strategic Imperative." *Crosstalk*, July 2009. http://www.stsc.hill.af.mil/CrossTalk/2006/07/0607Cartwright.html

Chambers, John (2009). *Building the Next Generation Company: Innovation, Talent, Excellence*. Lecture Delivered at the Massachusetts Institute of Technology, Cambridge, Massachusetts, 07 January 2009. http://blog.wirearchy.com/2009/01/07/john-chambers-ceo-of-cisco-at-mit-on-enterprise-20/

Collings, Deirdre, and Rafal Rohozinski (2009). *Bullets & Blogs—New Media and the Warfighter*. Carlisle Barracks, Pennsylvania: United States Army War College.

Cordesman, Anthony (2006). *Preliminary "Lessons" of the Israeli-Hezbollah War*. Washington, D.C.: Center for Strategic and International Studies.

Defense Industry Daily (2005). "Four-Star Blogging at STRATCOM." *Defense Industry Daily*, 28 March 2005. http://www.defenseindustrydaily.com/fourstar-blogging-at-stratcom-0239/

Doyne, Thomas A., Mike Hurley, and Thom Davis (2006). "Network-Enabled Program Management: Meeting the Space Acquisition Challenge." *High Frontier* Vol. 2 No. 2, 51–55.

Fox, S. G. (1995). *Unintended Consequences of Joint Digitization*. Newport, Rhode Island: United States Naval War College.

Goulding, Vincent (2009). “The Rifle Company Experiment,” *Marine Corps Gazette*, Dec. 2009, 67–69.

Graham, Paul (2005). *Web 2.0*. http://www.paulgraham.com/web20.html

Grant, Greg (2009). “Small Units Need Big Data Pipes,” *DoD Buzz*, 10 December 2009, http://www.dodbuzz.com/2009/12/10/small-units-need-big-data-pipes/

Jackson, Brian A. (2006). “Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and its Application to Al Qaeda.” *Studies in Conflict & Terrorism*, Vol. 29, 241–262.

Johnston, P. (2000). “Doctrine is not Enough: The Effect of Doctrine on the Behavior of Armies.” *Parameters, US Army War College Quarterly*, Autumn 2000, 30–39.

Jones, Seth G. (2007). “Fighting Networked Terrorist Groups: Lessons from Israel.” *Studies in Conflict & Terrorism*, Vol. 30, 281–302.

Jordan, Larry R. (2008). *Hybrid War: Is the U.S. Army Ready for the Face of 21st Century Warfare?* Fort Leavenworth, Kansas: U.S. Army Command and General Staff College.

Jordan, Javier, Fernando M. Manas, and Nicola Horsburgh (2008). “Strengths and Weaknesses of Grassroot Jihadist Networks: The Madrid Bombings.” *Studies in Conflict & Terrorism* Vol. 31, 17–39.

Koschade, Stuart (2006). “A Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence.” *Studies in Conflict & Terrorism* Vol. 29, 559–576.

Krulak, Charles C. (1999). “The Strategic Corporal: Leadership in the Three Block War.” *Marines Magazine* Vol. 28, No. 1. 32.

Oliveiro, Chuck (1998). “Trust, Manoeuvre Warfare, Mission Command, and Canada’s Army.” *Canadian Army Journal*, Vol. 1 No. 1.

Price, Robert R., and Jason A. McHuen (2009). Enabling Enhanced Company Operations (ECO): An Analysis of Tactical Communication Requirements and Solutions for a Marine Corps Company and Below. Monterey, California: Naval Postgraduate School.

Ramshaw, Ryan (2007). “C2-Less is More.” *Proc. 12th International Command and Control Research and Technology Symposium* (19–21 June, Newport, Rhode Island). Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org.

Rourke, Kellie S. (2009). *U.S. Counterinsurgency Doctrine: Is it Adequate to Defeat Hezbollah as a Threat Model of Future Insurgencies?* Fort Leavenworth, Kansas: U.S. Army Command and General Staff College.

Saunders, Clayton D. (2002). *Al Qaeda: An Example of Network-Centric Operations*. Newport, Rhode Island: United States Naval War College.

Senn, Matthew A., and James D. Turner (2008). *Analysis of Satellite Communication as a Method to Meet Information Exchange Requirements for the Enhanced Company Concept*. Monterey, California: Naval Postgraduate School.

Smith, Donald Steven (2006). "U.S. Must Network to Defeat al Qaeda, Kimmitt Says." Washington, D.C.: *American Forces Press Service*, 21 February 2006. http://www.defense.gov/news/newsarticle.aspx?id=14794

Soknich, William (2009). "Strategic Knowledge Integration Web (SKIWeb)-Global Awareness Presentation Services (GAPS)." *Proc. 2009 Commercial Joint Mapping ToolKit (CJMTK) Annual Conference*, 7 April, 2009. http://www.cjmtk.com/EventRegistration/CjmtkConf09/CJMTK_UC_2009_SKIWEB-GAPS.PDF

Stewart, Keith (2006). "Coalition Command and Control in the Networked Era." *Proc. 11th International Command and Control Research and Technology Symposium* (20–22 June, Cambridge, U.K.). Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org.

Stewart, Keith (2009). "Command Approach: Problem Solving in Mission Command." *Proc. 14th International Command and Control Research and Technology Symposium*, (15–17 June, Washington, D.C.). Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org.

Stulberg, Adam (2009). "Organizing for Revolutionary Effect: Managing the Many Faces of Network-Centric Operations." *Proc. International Studies Association Annual Convention*, New York, 15–18 Feb.

Talbot, David (2004). "How Technology Failed in Iraq." *Technology Review*, Nov. 2004.

Tan, David, Peter Thunholm, Lee Tin Hua, Per Wikberg, Ng Ee Chong, Ricky Chng, Esther Tan, Frederick Tey, Mikael Hallberg, and Sven-Ake Larsson (2009). "Edge Organization: Testing a New C2 Model of Battlefield Information Sharing and Coordination." *Proc. 14th International Command and Control Research and Technology Symposium*, (15–17 June, Washington, D.C.). Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD-NII), Command and Control Research Program (CCRP), www.dodccrp.org.

Thunholm, Peter, E.C. Ng, M. Cheah, K.Y. Tan, N. Chua, and C. L. Chua (2009). "Exploring Alternative Edge vs. Hierarchy C2 Organizations Using the ELICIT Platform with Configurable Chat System." *International C2 Journal* Vol. 3 No.2, 1–52.

UKArmy (2005*). Land Operations*. Shrivenham, UK: United Kingdom Ministry of Defence, Director General, Development, Concepts, & Doctrine, Publication AC 71819.

UKMoD (1989). *Design for Military Operations*. Shrivenham, UK: United Kingdom Ministry of Defence, Director General, Development, Concepts, & Doctrine, Publication AC 71451.

UKRAF (2008). *British Air and Space Power Doctrine* (AP3000 4th Edition). Cranwell, Lincolnshire, United Kingdom: Royal Air Force Center for Air Power Studies.

USAF (2007). *Command and Control*. Washington, D.C.: United States Air Force, Doctrine Document 2-8.

USArmy (2003). *Mission Command: Command and Control of Army Forces*. Washington, D.C.: Headquarters, United States Department of the Army, Field Manual No. 6-0.

USDoD (2008). 2008 National Defense Strategy. Washington, D.C.: United States Department of Defense.

USDoD (2009a). *Department of Defense Command & Control Strategic Plan* Version 1.0. Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense for Networks and Information Integration.

USDoD (2009b). *Department of Defense Command & Control Implementation Plan* Version 1.0. Washington, D.C.: United States Department of Defense, Office of the Assistant Secretary of Defense for Networks and Information Integration.

United States Joint Staff J-7 (2008). *Joint Capability Areas*. Washington, D.C.: United States Department of Defense, Joint Staff. http://www.dtic.mil/futurejointwarfare/strategic/jca101.ppt

USMC (1989). *Warfighting*. Washington, D.C.: Department of the Navy, Headquarters, United States Marine Corps, Publication FM 1.

USMC (1996). *Command and Control*. Washington, D.C.: Department of the Navy, Headquarters, United States Marine Corps, Doctrine Publication MCDP 6.

Vogelaar, L. W. and Eric Hanskramer (2004). “Mission Command in Dutch Peace Support Missions.” Armed Forces & Society Vol. 30 No. 3, 409–431.

Whine, Michael (1999). “Cyberspace—A New Medium for Communication, Command, and Control by Extremists.” Studies in Conflict & Terrorism Vol. 22, 231–245.

Wyld, David C. (2007). *The Blogging Revolution: Government in the Age of Web 2.0*. Washington, D.C.: IBM Center for the Business of Government.

Wyly, M. D. (1991). *Thinking like Marines*. http://www.belisarius.com/modern_business_strategy/wyly/thinking_like_marines.htm

Yardley, Ivan, and Andrew Kakabadse (2007). “Understanding Mission Command: a Model for Developing Competitive Advantage in a Business Context.” *Strat. Change* Vol. 16: 69–78.

Zagurski, Tyler J. (2004). *Direct, Plan, or Influence? Joint C2 on the Future Battlefield*. Quantico, Virginia: United States Marine Corps, Marine Corps University, School of Advanced Warfighting.

Zwikael, Ofer (2007). “Al Qaeda’s Operations: Project Management Analysis.” *Studies in Conflict & Terrorism* Vol. 30, 267–280.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE
January 2010

2. REPORT TYPE
Final

3. DATES COVERED *(From–To)*
September 2009 – January 2010

4. TITLE AND SUBTITLE

The Evolution Towards Decentralized C2

5a. CONTRACT NUMBER
DASW01-04-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

M.S. Vassiliou

5d. PROJECT NUMBER

5e. TASK NUMBER
AK-2-2701

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document NS D-4025
Log: H10 000112

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of the Director, Defense Research and Engineering
Information Systems
1777 North Kent Street
Rosslyn, VA 22209

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited. (26 March 2010)

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper examines (1) the degree to which the U.S. military is planning to move towards a more decentralized C2 paradigm; (2) the adoption of such a paradigm by adversaries; (3) the degree to which the United States is actually making the transition; and (4) the factors enabling and impeding the shift. We find that many adversaries of the West, including terrorist organizations and "hybrid enemies," are already operating in an agile, decentralized manner. Meanwhile, top-level strategic plans of the U.S. Department of Defense (DoD) are consistent with a transition to net-enabled decentralized command and control (C2) for the U.S. military where appropriate, and the shift is supported by stated mission command doctrine. The transition is already occurring to some degree. In Afghanistan, for example, small Marine units operate with significant autonomy and edge-like behavior. The DoD has also made progress in the use of web-enabled collaborative systems. These systems have broadened information distribution and stimulated new interaction patterns, although they have not changed the allocation of decision rights. Technologies enabling the shift to net-enabled decentralized C2 must be coupled with appropriate policies and procedures and occasionally must overcome mid-level institutional cultural resistance.

15. SUBJECT TERMS

command and control (C2), decentralized C2, net-centric C2, net-centric warfare, mission command doctrine, Web-enabled technologies

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Mr. David Jakubek
a. REPORT Uncl.	b. ABSTRACT Uncl.	c. THIS PAGE Uncl.	SAR	25	19b. TELEPHONE NUMBER *(include area code)* 703-588-7412